Nau a franchi depuis longtemps la frontière légale du piratage. Néanmoins, la Direction de la surveillance du territoire, occupée par plusieurs affaires de piratage de réseaux d'ordinateurs des facultés et des grandes écoles ne peut aider Surcouf. Il doit rassembler seul les preuves.

Puisque le forban est resté connecté alors que le système n'était plus relié physiquement au réseau de l'Internet, Surcouf soupçonne l'existence d'un modem piraté dans les bureaux. Son propre numéroteur téléphonique automatique découvre bientôt la brèche utilisée par Nau.

Il réinstalle alors sur son ordinateur d'administration un système propre, puis met en place un logiciel antipirates, nommé *T-Sight*, qui contrôle tous les ordinateurs du réseau de la société. Surcouf prépare également un piège : le logiciel *T-Sight* guettera la prochaine connexion sur admin.boucanier.fr et dirigera l'intrus sur un ordinateur «prison» où le coupable sera maîtrisé et identifié. Surcouf, avec une équipe de programmeurs, camoufle sa prison en un système multi-utilisateurs et y place des données financières factices en guise d'appât.

Le comble de l'orgueil

Deux jours plus tard, à 20 heures 17, quelqu'un s'introduit dans l'ordinateur admin.boucanier.fr. C'est Nau! Pourquoi est-il revenu si tôt? Nau a beaucoup apprécié – il en a même ri aux larmes – que les pirates de l'informatique et les chaînes de télévision parlent de ses talents. Il se sent invincible. Erreur...

Trop pressé, il se connecte sans les précautions habituelles sur pemmican.fr, puis sur l'ordinateur fantasia. Appâté par le leurre, il se dirige rapidement vers la prison. Au comble de l'excitation, il examine ce qu'il croit être des données financières importantes.

De son côté, Surcouf analyse rapidement les informations fournies par le programme *T-Sight* et obtient le mot de passe que Nau utilise pour pirater fantasia. Il suit ainsi l'intrus jusqu'à pemmican.fr. L'administratrice de ce réseau, prévenue au restaurant par son téléphone portable, contacte Surcouf.

Pendant que Nau recopie un énorme fichier contenant des numéros de cartes bancaires factices, Surcouf installe un programme *Sniffer* sur pemmican.fr. et consulte le compte de Nau dans cet ordinateur, car il a négligemment utilisé le même mot de passe pour tous ses comptes. Quelques minutes avant que Nau ait fini de recopier le fichier et se déconnecte, Surcouf retrouve le fichier de cartes bancaires volé sur le compte souscrit par Nau.

Les informations obtenues suffisent à la Direction de la surveillance du territoire, qui contacte le fournisseur et obtient l'identité de Nau. Munie de ces preuves, dont les comptes rendus détaillés fournis par le programme *Etherpeek*, le bureau du juge d'instruction délivre un mandat d'arrêt.

L'appartement de Nau est perquisitionné, et son ordinateur confisqué. Le disque dur de l'ordinateur révélera tout, même ce qui a été effacé. Un laboratoire identifie ses violations passées, notamment celle d'une grande institution bancaire parisienne.

Nau est mis en examen pour piratage informatique. Au procès, face à une juge intransigeante, Nau tente de négocier un compromis, malgré les dizaines de milliers de francs de dégâts occasionnés. Peine perdue, Jean Nau, dit l'Olonnais, purge aujourd'hui une peine de deux ans d'emprisonnement.

Carolyn MEINEL est écrivain scientifique spécialiste du piratage informatique.

Philippe BLANCHARD, *Pirates de l'informatique : enquête sur les hackers français*, Vuibert, 1995.

Æleen FRISCH, *Les bases de l'administration système*, deuxième édition, O'Reilly, 1996.

Jean GUISNEL, *Guerres dans le cyberespace*, Découverte, 1997.

Craig HUNT, *TCP/IP, Administration de réseau*, deuxième édition, O'Reilly, 1998.

Cryptographie et réseau

PHILIP ZIMMERMANN

Les courriers électroniques et les diverses informations numériques envoyées sur le réseau Internet sont comme des cartes postales numériques : leur contenu n'est pas protégé. Des systèmes de cryptographie assurent le secret des transmissions électroniques.

L'acheminement des lettres par la poste prend parfois des jours, mais les enveloppes cachent le contenu des messages. À l'inverse, le courrier électronique arrive en un clin d'œil, mais il peut être lu par des indiscrets. Des systèmes de chiffrement peuvent toutefois assurer la confidentialité de telles transmissions : on mélange l'information de manière tellement complexe qu'elle devient inintelligible, excepté pour le destinataire légitime, qui connaît les règles du mélange.

Depuis les années 1980, les ordinateurs personnels sont si puissants qu'ils peuvent utiliser des systèmes cryptographiques naguère réservés aux militaires. Ces systèmes, très efficaces, résistent à toute tentative de «cassage».

Sortir de l'ombre

Avant le milieu des années 1970, l'Agence de sécurité américaine (NSA pour *National Security Agency*) avait le quasi-monopole de la cryptographie américaine ; les méthodes étaient confidentielles, connues seulement de quelques «hommes du chiffre». En 1976, un article intitulé *De nouvelles voies pour la cryptographie*, a ouvert la cryptographie